Guidance for Implementation of the Judicial Conference Policy on Privacy and Public Access to Electronic Criminal Case Files

In September 2001, the Judicial Conference of the United States adopted a policy on privacy and public access to electronic case files (JCUS-SEP/OCT 01, pp. 48-50). This policy addressed civil, criminal, bankruptcy and appellate case files separately. With regard to criminal case files, the policy prohibited remote public access to criminal case files at that time, with the explicit statement that the Conference would revisit this issue within two years. In March 2002, the Judicial Conference approved the establishment of a pilot project that would allow 11 courts, ten district courts and one court of appeals, to provide remote electronic public access to criminal case files (JCUS-MAR 02, p. 10). A study of these courts conducted by the Federal Judicial Center outlined the advantages and disadvantages of such access, to court employees, the bar, and the public. The study did not reveal any instances of harm due to remote access to criminal documents. The results of the study were reported to the Committees on Court Administration and Case Management and Criminal Law.

The Committee on Court Administration and Case Management reviewed and discussed the study in depth, ultimately concluding that the benefits of remote public electronic access to criminal case file documents outweighed the risks of harm such access potentially posed. This decision was based not only on the results of the FJC study, but also on the extensive information the Committee, through its Privacy Subcommittee, gathered and evaluated during the period of deliberation that led to the Judicial Conference's adoption of the initial privacy policy in September 2001. That process included the receipt of 242 comments from a wide variety of interested persons including private citizens, privacy advocacy groups, journalists, attorneys, government agencies, private investigators, data re-sellers and members of the financial services industry. It also included a public hearing at which 15 individuals representing a wide spectrum of public, private, and government interest made oral presentations and answered questions from Privacy Subcommittee members.

From the comments received and presentations made, it was clear that remote electronic access to public case file information provides numerous benefits. Specifically, several speakers noted that such access provides citizens the opportunity to see and understand the workings of the court system, thereby fostering greater confidence in government. The benefit that electronic access

"levels the geographic playing field" by allowing individuals not located in proximity to the courthouse easy access to what is already public information was also frequently mentioned. Others noted that providing remote electronic access to this same public information available at the courthouse would discourage the creation of a "cottage industry" by individuals who could go to the courthouse, copy and scan information, download it to a private website and charge for access, thus profiting from the sale of public information and undermining restrictions intended to protect privacy.

After thoroughly analyzing and weighing all of the information before it, in June 2003, the Committee on Court Administration and Case Management recommended that the Judicial Conference amend its prohibition on remote public access to electronic criminal case files, the amendment to become effective only after specific guidance for the courts was developed. The Committee on Criminal Law concurred in this recommendation.

At its September 2003 session, the Conference discussed the issue and adopted the recommendation, thereby amending its policy regarding remote public access to electronic criminal case file documents to permit such access to be the same as public access to criminal case file documents at the courthouse with the effective date of this new policy delayed until such time as the Conference approves specific guidance on the implementation and operation of the policy developed by the Committees on Court Administration and Case Management, Criminal Law and Defender Services (JCUS-SEP 03, pp. 15-16).

This guidance, which was prepared by a specially-created subcommittee consisting of members from the Committees on Court Administration and Case Management, Criminal Law and Defender Services and approved by the Judicial Conference, sets forth the implementation guidelines required by the Judicial Conference. This document has three parts. The first provides a short explanation of the policy on remote public access to electronic criminal case files and explains how it relates to similar policies for other case types. The second part provides information about the redaction requirements which are an integral part of the policy and require the court to educate the bar and other court users. The third part is a discussion of specific documents that courts are not to make available to the public.

I. Explanation of the policy permitting remote public access to electronic criminal case file documents

Not all documents associated with a criminal case are properly included in the

criminal case file. The policy regarding remote public electronic access to criminal case file documents is intended to make all case file documents that are available to the public at the courthouse available to the public via remote, electronic access if a court is making documents remotely, electronically available through the Case Management/Electronic Case Files system or by the scanning of paper filings to create an electronic image. Simply stated, if a document can be accessed from a criminal case file by a member of the public at the courthouse, it should be available to that same member of the public through the court's electronic access system. This is true if the document was filed electronically or converted to electronic form.

This policy treats criminal case file documents in much the same way civil and bankruptcy case file documents are treated. Filers of documents have the obligation to partially redact specific personal identifying information from documents before they are filed. (See Section II, below for a discussion of redaction requirements.) However, because of the security and law enforcement issues unique to criminal case file information, some specific criminal case file documents will not be available to the public remotely or at the courthouse. (See Section III, below for a discussion of these documents.) It is not the intent of this policy to expand the documents that are to be included in the public criminal case file and, thereby, available both at the courthouse and electronically to those with PACER access.

It should also be noted that at its September 2003 session, the Judicial Conference adopted a policy that provides for the electronic availability of transcripts of court proceedings. The effective date of this policy is delayed pending a report of the Judicial Resources Committee regarding the impact the policy may have on court reporter compensation. However, once that policy becomes effective, there are separately articulated requirements and procedures regarding redaction which will apply to transcripts in criminal cases.

II. **Redaction and Sealing Requirements**

The policy adopted by the Conference in September 2003 states in part:

> Upon the effective date of any change in policy regarding remote public access to electronic criminal case file documents, require that personal data identifiers be redacted by the filer of the document, whether the document is filed electronically or in paper, as follows:

1. Social Security numbers to the last four digits;
2. financial account numbers to the last four digits;
3. names of minor children to the initials;
4. dates of birth to the year; and
5. home addresses to city and state[.]

In order to inform all court users of these requirements, courts should post a Notice of Electronic Availability of Criminal Case File Documents on their websites and in their clerks' offices. An example of such a notice appears below. As part of the pilot project and study conducted by the Federal Judicial Center (FJC), participating courts were asked to implement similar redaction requirements and to inform all court users of these requirements. To assist in these requests, the participating courts were provided with a sample Notice of Electronic Availability of Criminal Case File Documents that was reviewed by a Subcommittee of the Committee on Court Administration and Case Management, with a representative from the Criminal Law Committee, that was working with the FJC on the study's design. It was suggested that the courts post this notice on their websites and in their clerks' offices in order to inform all filers and other court users that documents filed in criminal cases will be available to the general public on the Internet and that the filer has the obligation to redact the specified identifying information from the document prior to filing. A version of this notice, updated to reference the E-Government Act of 2002, is provided.

Please be informed that documents filed in criminal cases in this court are now available to the public electronically.

> You shall not include sensitive information in any document filed with the court. You must remember that any personal information not otherwise protected will be made available over the Internet via WebPACER. The following personal data identifiers must be partially redacted from the document whether it is filed traditionally or electronically: Social Security numbers to the last four digits; financial account numbers to the last four digits; names of minor children to the initials; dates of birth to the year; and home addresses to the city and state.
>
> In compliance with the E-Government Act of 2002, a party wishing to file a document containing the personal data identifiers specified above may file an unredacted document under seal. This document shall be retained by the court as part of the record. The court may, however, also require the party to file a redacted copy for the public file.

Because filings will be remotely, electronically available and may contain information implicating not only privacy but also personal security concerns, exercise caution when filing a document that contains any of the following information and consider accompanying any such filing with a motion to seal. Until the court has ruled on any motion to seal, no document that is the subject of a motion to seal, nor the motion itself or any response thereto, will be available electronically or in paper form.

1) any personal identifying number, such as driver's license number;
2) medical records, treatment and diagnosis;
3) employment history;
4) individual financial information;
5) proprietary or trade secret information;
6) information regarding an individual's cooperation with the government;
7) information regarding the victim of any criminal activity;
8) national security information; and
9) sensitive security information as described in 49 U.S.C. § 114(s).

Counsel is strongly urged to share this notice with all clients so that an informed decision about the inclusion of certain materials may be made. If a redacted document is filed, it is the sole responsibility of counsel and the parties to be sure that all documents and pleadings comply with the rules of this court requiring redaction of personal data identifiers. The clerk will not review filings for redaction.

The court should also be aware that it will need to partially redact the personal identifiers listed above from documents it prepares that routinely contain such information (e.g., order setting conditions of release).

III. **Documents for which public access should not be provided**

The following documents shall not be included in the public case file and should not be made available to the public at the courthouse or via remote electronic access:

- unexecuted summonses or warrants of any kind (e.g., search warrants, arrest warrants);
- pretrial bail or presentence investigation reports;
- statements of reasons in the judgment of conviction;
- juvenile records;
- documents containing identifying information about jurors or potential jurors;
- financial affidavits filed in seeking representation pursuant to the Criminal Justice Act;
- ex parte requests for authorization of investigative, expert or other services pursuant to the Criminal Justice Act; and
- sealed documents (e.g., motions for downward departure for substantial assistance, plea agreements indicating cooperation)

Courts maintain the discretion to seal any document or case file sua sponte. If the court seals a document after it has already been included in the public file, the clerk shall remove the document from both the electronic and paper public files as soon as the order sealing the document is entered. Counsel and the courts should appreciate that the filing of an unsealed document in the criminal case file will make it available both at the courthouse and by remote electronic access. Courts should assess whether privacy or law enforcement concerns, or other good cause, justify filing the document under seal.

There are certain categories of criminal case documents that are available to the public in the clerk's office but will not be made available electronically because they are not to be included in the public case file for individual criminal cases. These include but are not limited to vouchers for claims for payment, including payment for transcripts, (absent attached or supporting documentation) submitted pursuant to the Criminal Justice Act. (For detailed guidance about the public availability of Criminal Justice Act information, please see paragraph 5.01 of Volume VII of *Guide to Judiciary Policies and Procedures.*)

Model Local Rule Regarding
Privacy and Public Access to Electronic Criminal Case Files

In compliance with the policy of the Judicial Conference of the United States,

and the E-Government Act of 2002, and in order to promote electronic access to documents in the criminal case files while also protecting personal privacy and other legitimate interests, parties shall refrain from including, or shall partially redact where inclusion is necessary, the following personal data identifiers from all documents filed with the court, including exhibits thereto, whether filed electronically or in paper, unless otherwise ordered by the court.

a. **Social Security numbers**. If an individual's Social Security number must be included, only the last four digits of that number should be used.
b. **Names of minor children**. If the involvement of a minor child must be mentioned, only the initials of the child should be used.
c. **Dates of birth**. If an individual's date of birth must be included, only the year should be used.
d. **Financial account numbers**. If financial account numbers are relevant, only the last four digits of the number should be used
e. **Home addresses**. If a home address must be included, only the city and state should be listed.

In compliance with the E-Government Act of 2002, a party wishing to file a document containing the personal data identifiers listed above may file an unredacted document under seal. This document shall be retained by the court as part of the record. The court, may, however, still require the party to file a redacted copy for the public file.

The responsibility for redacting these personal identifiers rests solely with counsel and the parties. The clerk will not review filings for compliance with this rule.

COMMENTARY

Parties should consult the "Guidance for Implementation of the Judicial Conference Policy on Privacy and Public Access to Electronic Criminal Case Files." This Guidance explains the policy permitting remote public access to electronic criminal case file documents and sets forth redaction and sealing requirements for documents that are filed. The Guidance also lists documents for which public access should not be provided. A copy of the Guidance is available at the court's website.